Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

1030 Wien, Seidlgasse 22 / 9
Tel.: +43 1 503 19 63-0
Fax: +43 1 503 19 63-66

8010 Graz, Inffeldgasse 16a
Tel.: +43 316 873-5514
Fax: +43 316 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

QSCD-Certificate
pursuant to Art. 30 para. 3 lit. b eIDAS[1]

Qualified Signature and Seal Creation Device (QSCD) NITROXIII CNN35XX-NFBE HSM Family, version 2.09

Applicant:
Marvell Semiconductor, Inc.
5488 Marvell Lane
Santa Clara, CA 95054
U.S.A.

Reference number: A-SIT-VIG-19-078

QSCD-Certificate valid from:
See Date of Qualified Electronic Signature

1. Product Description

The hereby certified product “Qualified Signature and Seal Creation Device (QSCD) NITROXIII CNN35XX-NFBE HSM Family, version 2.09” (also denoted as “Marvell LS1 HSM” or “Marvell LiquidSecurity® HSM”) by Marvell Semiconductor, Inc., is a Qualified Remote Signature/Seal Creation Device (QSCD). It provides a remote signature and seal creation service, where none of the QSCD’s components are on the client side but deployed in the tamper-protected environment of the Trust Service Provider (TSP). When operated by a Qualified Trust Service Provider (QTSP), and used in conjunction with qualified certificates as well as a suitable Server Signing Application (SSA) and a Signature Creation Application (SCA) either (1) qualified electronic signatures or (2) qualified electronic seals as defined in eIDAS (amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024) can be created with the legal effects of (1) Article 25 resp. (2) Article 35 when.

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024

Subcomponents:

The QSCD consists of the NIST FIPS 140-3 level 3 certified NITROX III CNN35XX-NFBE Cryptographic Module (HSM – Hardware Security Module) in the form of a PCIe[2] card and the SAM (Signature Activation Module). The SAM is a software that is integrated into the Firmware of the HSM and both form the QSCD, hence the certification scope. The QSCD is intended to be operated by a qualified trust service provider (QTSP) in a controlled environment according to its FIPS 140-3 level 3 certification in conjunction with the corresponding Security Policy and necessarily activating the so-called “eIDAS mode” of that HSM. That particular eIDAS mode can be enabled during the initialization of the partition. Once the QSCD is initialized without the eIDAS mode being activated, it cannot be enabled thereafter.

The HSM is a tamper-proof hardware component and it is used as a cryptographic module for the generation and protection of the signature and seal creation data (SCD). Moreover, it is responsible for storing all cryptographic keys that are used for the creation of both qualified electronic signatures and qualified electronic seals. The HSM provides all cryptographic operations to establish an end-to-end secure tunnel between the remote SCA and the host and between the host and the QSCD, this secure tunnel is required to use signature or seal creation data hence create both qualified electronic signatures or qualified electronic seals. The host is operated in the secure environment of a QTSP.

The HSM can be used as an embedded standalone device to be inserted in a server or as an embedded component in a Marvell LiquidSecurity® Appliance[3]. The physical boundary of the QSCD is the outer perimeter of the PCIe card itself. That means that the LiquidSecurity® Appliance is not in the scope of this QSCD certification.

For the successful deployment of the HSM as a QSCD, the HSM must be integrated with at minimum a 3rd party signature creation application (SCA) and where required a server signing application (SSA). These components (SCA, SSA) are outside of the scope of this certification.

Generation of Signature and Seal Creation Data:

The Signature or Seal Creation Data (SCD) is generated and stored within the HSM. Both long-time (also denoted as “long-term”) and one-time keys can be generated inside of the HSM and those can be used for the SCD.

Following the generation of the SCD, the corresponding public key is extracted from the HSM to support the creation of a qualified certificate. However, the creation of the Certificate Signing Request (CSR) alongside the resulting Qualified Certificate is out of scope of the certification.

The HSM includes up to 64 HSM partitions. The signatory or creator of a seal must be in control of the partition on the HSM that is used to store the key ahead of the generation request being issued. This is achieved by the signatory or creator of a seal initializing the login credentials for the target partition or key ahead of its use and thus perform an authentication.

Storage of Signature and Seal Creation Data:

The SCD are stored in a dedicated key storage of an HSM partition with both its confidentiality and integrity protected long-time by the HSM. In this context, the SCD is protected in a way such that

(i) the keys can only be used inside of the HSM;

(ii) the keys can only be used following a login to the target partition by the signatory or creator of a seal that is owning the SCD;

(iii) integrity protection for the keys is provided by the HSM throughout their life.

Where session-based keys are used, SCD is only stored by the HSM in volatile memory and is securely overwritten on active closure of the associated session.

[2] PCIe – Peripheral Component Interconnect Express

[3] The certified hardware and firmware versions of the used cryptographic modules, for which this QSCD certificate is valid, are given in Section 6.

Signature and Seal Creation:
The signatory or the creator of a seal interacts with the QSCD using a device (e.g., laptop, smart phone or tablet) via the Server Signing Application (SSA). The purpose of the interaction between the device and the SSA is for the signatory or for the creator of a seal to utilize the SSAs signing service.

To ensure that the signatory of the creator of a seal has the sole control of the legitimately used signing/sealing keys, the signature/sealing operation needs to be authorized. This is performed by the Signature Activation Module (SAM) to activate the signing key inside of the used Cryptographic Module (i.e., the HSM). The HSM enforces a model for session-based controls on authorization to both access and use the SCD.

Ahead of using the SCD, the signatory or the creator of a seal must be successfully authenticated to the target partition. Once the signatory or the creator of a seal has been authenticated, either the Data To Be Signed (DTBS) or the DTBS/representation (DTBS/r) is sent to the HSM for signing or for sealing. The signature operation is performed using a Signature Activation Protocol (SAP). The SAP requires that the Signature Activation Data (SAD) are to be provided at the local environment by the signatory or by the creator of the seal. The SAD binds the signatory or the creator of a seal authentication data with the signing key (or the sealing key) and the data to be signed (DTBS/R(s)).

Once the signature or the seal is received, the session is closed.

Where one-time keys are used, the SCD creation and public key extraction alongside the signature or seal creation must occur within a single session. After the creation of the signature or of the seal this session hence must be deactivated.
All sessions with active partitions must be performed using the QSCD supplied cryptographically secured tunnel which is to be identified as an ‘encrypted communication channel’. This encrypted communication channel provides an additional layer of authentication of the remote client on the one hand and on the other hand confidentiality, integrity and replay protection for traffic during the signature or seal creation request.

2. Compliance with the Requirements of eIDAS

The QSCD meets the following requirements, provided that the conditions in section 4 are fulfilled:

- requirements laid down in Article 29 para 1[4] eIDAS,
- requirements laid down in Article 39 para 1[5] eIDAS,

[4] *Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.*
[5] *Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.*

- requirements laid down in Annex II eIDAS (para 1 lit. a[6],b[7],c[8],d[9], para 2[10], para 3[11], para 4 lit a[12], b[13])

The compliance of the QSCD is thus confirmed within the following categories:

- components and procedures for the generation of signature or seal creation data,
- components and procedures for the storage of signature or seal creation data,
- components and procedures for the processing of signature or seal creation data

3. Validity Period of the QSCD-Certificate

This QSCD-Certificate is valid up to 5 years or until revocation by A-SIT.

On assignment A-SIT will conduct a continuous surveillance concerning the security of the technical components and processes used as well as the suitability of the cryptographic algorithms and parameters. The issuance of this QSCD-Certificate includes surveillance for a period of two years. In order to maintain a valid certification, the applicant has to conduct a vulnerability assessment every two years and remedy any identified vulnerabilities in a timely manner. The QSCD-Certificate will be revoked if the technical components and processes or the cryptographic algorithms and parameters used no longer reflect the state of the art, if vulnerability assessments are not conducted every two years, or if identified vulnerabilities are not remedied in a timely manner or if there is no further surveillance assigned.

4. Operating Conditions

The validity of this QSCD-Certificate is subject to the conditions stated below. The measures taken shall be

- ascertained by the trust service provider’s security and certification policy,
- integrated into the guidance of the signatory or creator of a seal and
- their effect shall be ensured by means of supervision (in accordance with Article 20 eIDAS).

[6] *Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured.*

[7] *Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that the electronic signature creation data used for electronic signature creation can practically occur only once.*

[8] *Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology.*

[9] *Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.*

[10] *Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.*

[11] *Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.*

[12] *Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met: the security of the duplicated datasets must be at the same level as for the original datasets.*

Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met: the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.

(1) The unambiguous assignment and the safe completion of the user session, the confidentiality and integrity of the authorization codes as well as the integrity of the data to be signed or to be sealed during transmission from the signatory or creator of a seal to the QSCD are part of the QSCD's system environment[14] and thus outside the scope of this QSCD-certificate. It must be ensured that the signatories or creators of a seal are informed that components used for the initiation of the signature or sealing process (OTP device, mobile phone, web browser) must be suitably protected. The signatories shall keep control of their assigned OTP devices and shall promptly report any circumstance where the credential is compromised according to the defined revocation or suspension procedures.

(2) The QSCD must be operated by a qualified trust service provider (QTSP).

(3) The qualified trust service provider must operate the QSCD in a protected environment, in particular:

- physical access to the QSCD is limited to authorized privileged users
- the QSCD or any of its externally stored assets are protected against loss or theft
- the QSCD is regularly inspected to deter and detect tampering (including attempts to access side-channels, or to access connections between physically separate parts of the QSCD, or parts of the hardware appliance)
- the QSCD is protected against the possibility of attacks based on emanations (e.g. electromagnetic emanations) according to risks assessed for the operating environment
- the QSCD is protected against unauthorized software and configuration changes
- all instances of the QSCD holding the same assets (e.g. where a key is present as a backup in more than one instance of the QSCD) are protected to an equivalent level

(4) During HSM initialisation the principle of dual control must be ensured and at least one person must have the role "Master Crypto Officer". For further administrative tasks during the operation the principle of dual control must be ensured. During its initialization the HSM must be switched to FIPS 140-3 approved mode. To guarantee dual control at least two distinct persons shall be used as HSM activation data holders to configure the HSM and the partition inside the HSM used for the SCD.

(5) Electronic signature or seal creation data may be duplicated for back-up purposes only to the extent strictly necessary to ensure continuity of the service.

(6) Only those cryptographic algorithms, key sizes and hash functions listed in section five shall be used for the creation of qualified electronic signatures or qualified electronic seals.

(7) External authentication mechanisms, which are used to authenticate a user in order to create a qualified electronic signature or seal, shall correspond to an authentication means equivalent to EC Implementing Regulation 2015/1502 for assurance level substantial or high[15].

(8) It must be ensured that components of signatories (or creators of a seal), which have vulnerabilities or are otherwise not suitable for authentication, cannot be used to authorize a signature creation.

5. Algorithms and Corresponding Parameters

For the creation of qualified electronic signatures or qualified electronic seals the QSCD uses the cryptographic algorithms

[14] in accordance with recital 56 of eIDAS

[15] COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market; as defined in ANNEX Clauses 2.1, 2.2.1 and 2.3.1

- RSASSA-PKCS1-v1_5[16] or RSASSA-PSS according to PKCS#1 v2.2 (RFC 8017 and FIPS 186-4) with cryptographic key size 2048-bit[17], 3072-bit or 4096-bit according to PKCS#1 v2.2 (RFC 8017 and FIPS 186-4) with cryptographic key sizes 2048-bit[17], 3072-bit or 4096-bit
- ECDSA[18] using the curves P-256, P-384 or P-521 of the NIST family according to FIPS 186-4 with cryptographic key sizes from 256-bit to 512-bit alongside brainpool_p256r1, brainpool_p384r1, brainpool_512r1 as per RFC 5639 with cryptographic key sizes from 256-bit to 512-bit as well as FRP256v1 according to ANSSI[19].

For the calculation of hash values, the hash functions SHA2-256, SHA2-384, SHA2-512 according to FIPS 180-4 are supported.

6. Assurance Level and Strength of Mechanism

For the used HSM NITROXIII CNN35XX-NFBE the following NIST FIPS 140-3 validation certificate issued by the US (National Institute of Standards and Technology) and the Canadian (Communications Security Establishment) FIPS 140 series certification body applies. The certificate confirms that the HSM was successfully evaluated against FIPS 140-3 level 3:

- Certificate #4700 issued on 2024-05-30 for NITROXIII CNN35XX-NFBE HSM Family; Firmware Versions: CNN35XX-NFBE-FW-2.09-0702, CNN35XX-NFBE-SMW-2.09-0702, CNN35XX-UBOOT-4.03-03; Hardware Version: HW-1.0 (CNL3510-NFBE-G; CNL3510P-NFBE-G; CNL3530-NFBE-G; CNL3560-NFBE-G; CNL3560P-NFBE-G; CNN3510-NFBE-G; CNN3530-NFBE-G; CNN3560-NFBE-G; CNN3560P-NFBE-G); HW-2.0 (CNL3510-NFBE-2.0-G; CNL3510B-NFBE-2.0-G; CNL3510P-NFBE-2.0-G; CNL3510PB-NFBE-2.0-G; CNL3530-NFBE-2.0-G; CNL3530B-NFBE-2.0-G; CNL3560-NFBE-2.0-G; CNL3560B-NFBE-2.0-G; CNL3560P-NFBE-2.0-G; CNL3560PB-NFBE-2.0-G; CNN3505LP-NFBE-2.0-G; CNN3510-NFBE-2.0-G; CNN3510LP-NFBE-2.0-G; CNN3510LPB-NFBE-2.0-G; CNN3530-NFBE-2.0-G; CNN3560-NFBE-2.0-G; CNN3560P-NFBE-2.0-G); HW-3.0 (CNL3510-NFBE-3.0-G; CNL3510A-NFBE-3.0-G; CNL3510C-NFBE-3.0-G; CNL3510D-NFBE-3.0-G; CNL3510E-NFBE-3.0-G; CNL3510F-NFBE-3.0-G; CNL3510I-NFBE-3.0-G; CNL3510P-NFBE-3.0-G; CNL3530-NFBE-3.0-G; CNL3530A-NFBE-3.0-G; CNL3530B-NFBE-3.0-G; CNL3530C-NFBE-3.0-G; CNL3530D-NFBE-3.0-G; CNL3530E-NFBE-3.0-G; CNL3530F-NFBE-3.0-G; CNL3560-NFBE-3.0-G; CNL3560A-NFBE-3.0-G; CNL3560B-NFBE-3.0-G; CNL3560B-NFBE-3.0-G-FB; CNL3560C-NFBE-3.0-G; CNL3560D-NFBE-3.0-G; CNL3560E-NFBE-3.0-G; CNL3560F-NFBE-3.0-G; CNL3560P-NFBE-3.0-G; CNN3505LP-NFBE-3.0-G; CNN3505LPA-NFBE-3.0-G; CNN3505LPC-NFBE-3.0-G; CNN3505LPD-NFBE-3.0-G; CNN3505LPE-NFBE-3.0-G; CNN3505LPF-NFBE-3.0-G; CNN3510-NFBE-3.0-G; CNN3510A-NFBE-3.0-G; CNN3510C-NFBE-3.0-G; CNN3510D-NFBE-3.0-G; CNN3510E-NFBE-3.0-G; CNN3510F-NFBE-3.0-G; CNN3510LP-NFBE-3.0-G; CNN3510LPA-NFBE-3.0-G; CNN3510LPB-NFBE-3.0-G; CNN3510LPC-NFBE-3.0-G; CNN3510LPD-NFBE-3.0-G; CNN3510LPE-NFBE-3.0-G; CNN3510LPF-NFBE-3.0-G; CNN3530-NFBE-3.0-G; CNN3530A-NFBE-3.0-G; CNN3530C-NFBE-3.0-G; CNN3530D-NFBE-3.0-G; CNN3530E-NFBE-3.0-G; CNN3530F-NFBE-3.0-G; CNN3560-NFBE-3.0-G; CNN3560A-NFBE-3.0-G; CNN3560C-NFBE-3.0-G; CNN3560D-NFBE-3.0-G; CNN3560E-NFBE-3.0-G; CNN3560F-NFBE-3.0-G; CNN3560P-NFBE-3.0-G)

[16] Annotation: The acceptability deadline for the legacy use of PKCS1-1_5 is set to December 31, 2030, by *"SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms",* Version 1.3, February 2023

[17] Annotation: The acceptability deadline for the legacy use of modulus of size above 1900 bits, but less than 3000 bits, is set to December 31, 2025 by *"SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms",* Version 1.3, February 2023

[18] ECDSA – Elliptic Curve Digital Signature Algorithm

[19] ANSSI *"Avis relatif aux paramètres de courbes ellitpiques définis pas l'État français"*. In: Journal Officiel 0241 (Oct. 2011), p. 17533 as referenced in *"SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms",* Version 1.3, February 2023 [Accessed: 21.10.2024]

Since there are no standards for the security assessment published by the European Commission by means of implementing acts, the QSCD certification was performed under eIDAS article 30 para 3. lit b amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 and the confirmation body applied comparable security levels considering the current state of the art.

In its intended environment the QSCD resists against attackers with high attack potential.

The results of the performed assessment which is the basis for this QSCD-Certificate are documented in the QSCD-Certification report under the reference A-SIT-VIG-19-078.

Authorized Signature:

A-SIT Secure Information Technology Center – Austria

Vienna, (Date see electronic signature)

SIGNATURE INFORMATION	**Signatory**	Herbert Leitold
	Date/Time-UTC	2024-10-21T21:57:17+02:00
	Verification	Information about the verification of the electronic signature can be found at: https://www.signaturpruefung.gv.at

Herbert Leitold, Director